Uwe Krause

(wip) Noch kein Titel

Fakultät Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Inhaltsverzeichnis

1 Motivation & Einleitung

1.1 Motivation: IT-(un)sicherheit allgemein

- (todo: aktuelle Quelle/Referenz)

1.2 Ziel: Programmierer verbessern

- Unsicherheit „greifbar“ machen
- um für die Einhaltung von „Secure coding Vorgaben“ / „best practices“ zu werben
  - (todo: Referenz??)
- (nicht Pentester ausbilden)

1.3 Didaktische Basis

- Blooms (revisited) Taxonomy [1]
- ICAP (Interactive - Constructive - Active - Passive) [2]

1.4 Vorgehen:

ctf als Elemente aus Pentester-„Ausbildung“ nutzen für Security Awareness bei Programmierern

- ctf as serious game
  - Designing a Serious Game for Cybersecurity Education [3]
  - Software Engineering for Games in Serious Contexts [4]

1.5 Diese Arbeit: Aufbau einer Beispiel-Challenge

In dieser Arbeit wird eine Beispiel-Challenge aufgebaut

1.5.1 Anforderungen an eine Challenge

- On the Requirements for Serious Games geared towards Software Developers in the Industry [5]

1.5.2 Evaluation

- Erfüllungsgrad der Anforderungen
- Vergleich mit anderen CTF
  - (Werte für andere CTF nicht selbst ermittelt: entommen aus Anforderungspaper)

2 Didaktische Basis

Verschiedene didaktische Konzepte bekräftigen, dass Lernende am erfolgreichsten sind, wenn sie sich aktiv mit dem Lerngegenstand beschäftigen.

2.1 Blooms Taxonomie

In Blooms (überarbeiteter) Taxonomie etwa gibt es verschiedene aufeinander aufbauende Ebenen des Verständnis, oft dargestellt als eine Pyramide. Die Basis bildet die Verständnis-Stufe des „Erinnerns“, der Fähigkeit relevantes Wissen aus dem Langzeitgedächtnis abzurufen. Darauf aufbauend folgt das „Verstehen“, das es ermöglicht Wissen zusammenzufassen, zu interpretieren, zu vergleichen und zu erklären. Nach der Stufe des selbst „Anwenden“, steht das Vermögen Sachverhalte zu „analysieren“, also das Material in seine Einzelteile zu zerlegen, übergreifende Struktur und Zweck zu ermitteln sowie Muster zu erkennen. Erst wer dazu in der Lage ist, wird auch „bewerten“ können, sich ein Urteil bilden und Bestehendes kritisieren können. An der Spitze der Taxonomie steht die Fähigkeit angeeignete Elemente zusammenzufügen, um Neues zu erschaffen. [1]

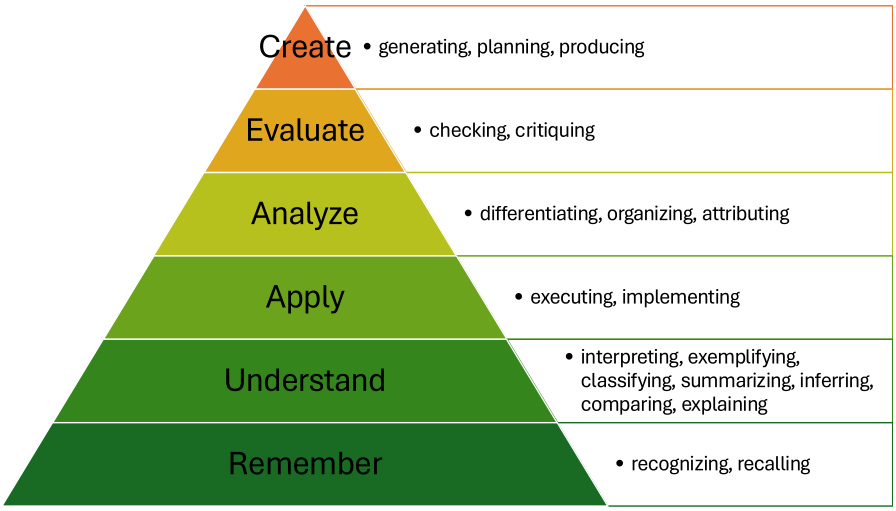

Abbildung 1: Blooms Pyramide, nach [1]. Eigene Darstellung

2.2 ICAP (Interactive - Constructive - Active - Passive)

Bei dem ICAP-Ansatz werden aufbauend auf dem Vorgehensmodell des „aktiven Lernens“ vier Modelle der kognitive Lernaktivitäten definiert und Wege vorgeschlagen, wie Wissensveränderungsprozesse angestoßen werden sollten. Zwar kann Wissen durch das passiven Empfangen von Informationen durch Zuhören oder Lesen aufgebaut werden, dies stellt aber die niedrigste Stufe dar. Die Wissensaufnahme kann aktiver gestaltet werden, zum Beispiel indem beim Zuhören zusätzlich Notizen gemacht werden oder beim Lesen Textstellen angestrichen werden und einzelne Passagen zusammengefasst werden. Konstruktives Verarbeiten ist über die Aufnahme von Erlerntem hinausgehendes Generieren von Dingen, beispielsweise wenn in einer Vorlesung Fragen gestellt werden oder zu einem beschriebenen Zusammenhang eine Zeichnung angefertigt wird. Die höchste Stufe des Modells ist die Interaktion mit dem Lerngegenstand, beispielsweise der Verteidigung eines Standpunkts in einer Gruppendiskussion bei der neue Ideen entstehen. Diesen vier Lernaktivitäten werden die jeweilig zu erwartenden kognitiven Ergebnisse gegenübergestellt: Passiv erlangtes Wissen kann im wörtlich und im gleichen Kontext wiedergegeben werden, wohingegen aktiv Erlangtes auf ähnliche Kontexte angewendet werden kann. Einmal generiertes Wissen kann in neuen Situationen angebracht werden, Kenntnis über das erlernte Konzept erlaubt Interpretation und Erklärungen, auch unter geänderten Rahmenbedingungen. Das tiefste Verständnis ist nach der Interaktion zu erwarten, potentiell können neue Produkte, Interpretationen und Ideen entstehen. [2]

2.3 Methoden der Wissensvermittlung

Die Essenz und das in diversen weiteren Ansätzen immer wieder zu beobachtender Lernmuster, ist die möglichst aktive Beschäftigung mit dem Lerngegenstand durch die Lernenden selbst. [6] Wenn Jura-Studierende Gerichtsurteile aufarbeiten, im Betriebswirtschaftsstudium Fallstudien bearbeitet werden und angehende Mediziner:innen anhand der Begutachtung von Leichen die Todesursache ermitteln [6], wie können Programmierer:innen sich mit den abstrakten Themen der IT-Sicherheit und sichererer Programmierung beschäftigen?

Wird versucht Konzepte der IT-Sicherheit über Vorträge oder Webinare zu IT-Sicherheit zu vermitteln, stellen diese (sofern sie denn überhaupt wahrgenommen werden; ungeteilte Aufmerksamkeit vorausgesetzt) lediglich die niedrigste Stufe der ICAP-Skala dar. Mehr als eine grundlegende Wissensaufnahme ist nicht zu erwarten, was im Bloomschen Modell ebenfalls der untersten Stufe entspricht. Eine aktivere Beschäftigung mit sicheren Programmiermethoden kann etwa bei Code reviews das Hervorheben von fehlerhaftem Code sein. Werden Problembereiche auf diese Art erkannt, entspricht dies dem „Verstehen“ auf der Bloomschen Skala. Es darf erwartet werden, dass das Wissen genug abstrahiert wurde, um eine Chance darauf zu haben, ähnliche Fehler in ähnlichen Kontexten wieder entdecken zu können. Um sich konstruktiv mit IT-Sicherheit zu beschäftigen, bieten sich sogenannte Hackathons an, bei denen Sicherheitsrelevante Systeme oder Komponenten entwickelt werden. Eine Person die bereits einmal etwa ein Login-System entworfen oder implementiert hat, wird benötigte Verfahren nicht nur angewendet haben, sondern wahrscheinlich das Wissen auch in seine Bestandteile zerlegt und zumindest Teile davon analysiert haben. Sie sollte diese Fähigkeit auch unter geänderten Rahmenbedingungen anwenden können. Um die Stufe des tiefsten Verständnis zu erreichen, ist die Interaktion mit einer Sicherheitslücke selbst angebracht, etwa durch das Verteidigen oder Angreifen eines Systems mit einer Sicherheitslücke. Hat eine Angreifer:in es geschafft, eine Sicherheitslücke selbst auszunutzen, hat sie bewiesen das Wissen nicht nur analysiert, sondern auch umfassend bewertet sowie mit dem erfolgreichem Angriff etwas erschaffen zu haben. Und sei dies nur in einer simulierten Umgebung geschehen, so darf trotzdem davon ausgegangen werden, dass das zugrundeliegende Problem wirklich verstanden wurde.

2.4 Serious Games ermöglichen Interaktion

Die skizzierte Form der Interaktion werden auch als „Serious Games“ bezeichnet. Allgemein werden diese entwickelt, um über reale Themen wie Gesundheitsfürsorge, Sicherheit oder Umweltfragen aufzuklären, zu schulen oder zu informieren. [4] Wenn Serious Games das Lernen komplexer und technischer Themen erleichtern, können Konzepte der IT-Sicherheit ebenfalls mit Techniken aus diesem Bereich vermittelt werden. In Lernumgebungen für konkrete zu lernende Konzepte der IT-Sicherheit stellen Spieler sich realistischen Herausforderungen. [3]

Werden auf diese Art IT-Security Techniken vermittelt, findet dies üblicherweise im Rahmen von „capture the flag“ (ctf) statt, einer Art IT-Security-Wettbewerb. Hier gibt es verschiedene Typen von Aufgaben („challenges“), beispielsweise im „Jeopardy-style“, bei dem es für gelöste Aufgaben in unterschiedlichen Kategorien Punkte zu gewinnen gibt. [7] Aufgaben in der Kategorie „Web“ beispielsweise bestehen häufig aus einem Webserver, der den Spielern eine Website mit einer oder mehreren absichtlich platzierten Schwachstellen zur Verfügung stellt. Diesen Webserver gilt es anzugreifen, indem die Sicherheitslücke(n) identifiziert und ausgenutzt werden. Üblicherweise ist zu beobachten, dass Teilnehmende großes Interesse am wettbewerbsorientierten Lernen zeigen [8] und „capture the flag“-Aufgaben die Interaktion von Lernenden mit dem Lerngegenstand erhöhen, was zu besser entwickelten Fähigkeiten im Umgang mit Sicherheitslücken führt [9].

Capture the Flag als Eigenart der Serious Games bieten Teilnehmenden eine Möglichkeit in einer extra hierfür bereitgestellten Umgebungen den Umgang mit Sicherheitslücken zu erlernen. Sie sind also ein geeignetes Mittel, um Kenntnisse im Bereich IT-Sicherheit zu vermitteln.

2.5 Anforderungen an serious games

Damit die eingesetzten Ressourcen möglichst optimal genutzt werden und der Interaktionsgegenstand auf das definierte Ziel einzahlt, müssen die Anforderungen an die Interaktionsumgebung klar formuliert sein. Für Serious Games die sich an praktizierende Software-Entwickelnde richten wurden durch Kombination akademischer und industrieller Forschung 15 Anforderungen[1] definiert. [5]

[1] Die Anforderungen werden gemeinsam mit der folgenden Evaluation in Tabelle 1 aufgelistet.

3 Interaktive Lernumgebung

Angelehnt an den ICAP-Ansatz wird im Folgenden eine interaktive Lernumgebung aufgebaut, mit dem Ziel Lernende für ein definiertes IT-Sicherheitsproblem zu sensibilisieren und ihnen zu ermöglichen, ähnliche Sicherheitslücken künftig zu erkennen und zu bewerten.

3.1 Lernziel („learning goal objective“)

3.1.1 Übergeordnet

Broken Access Control

- Top 1 der aktuellen OWASP “Top 10 Web Application Security Risks”.

3.1.2 Konkret

Direkter Zugriff

- Direkte Anfrage nach Ressourcen, die aus der GUI nicht erreichbar wären CWE-425
- Auslesen von Meta-Daten, trotz fehlender Zugriffsberechtigungen CWE-200

Rechte-Ausweitung

- Rechte-Ausweitung (innerhalb der Anwendung)
  - ermöglicht durch fehlende Authorisationsprüfung CWE-862
- Rechte-Ausweitung (innerhalb der Plattform)
  - Initial-Modus, aktiviert, wenn keine Anwender registriert sind. Der erste registrierte Account wird dann mit Administrationsrechten ausgestattet. Der Zugriff zu diesem initial-Modus ist nicht eingeschränkt CWE-1188.
  - In Kombination mit einem unsicheren Anwender-Verwaltungs-Endpunkt, der es ohne Autorisation CWE-306 erlaubt Anwender zu löschen, kann ein Angreifer alle bestehenden Anwender, inklusive des bestehenden Administrations-Anwenders, löschen, um anschließend einen neuen Account anzulegen. Diesem wird nun von der Anwendung Administrationsrechte zugesprochen.

3.2 Storyline der Challenge

3.2.1 Aus Sicht des Programmierers

- Reddit ist erfolgreich
  - Kritik: zu offen, alles für alle lesbar, Leute mischen sich ein

Also: Schaffen einer privaten Austauschplattform „Glesn“.

- Hauptkonzept: „Spaces“
  - Themenbezogene Erfahrungs-Austausch-Kreise
  - Zutritt nur auf Einladung (“invite only”)

Architektur

- Relationsmodell
  - User - Spaces - Artikel
- kurze Beschreibung Django
  - inklusive Besonderheit Django Admin

3.2.2 Aus Sicht des Betreibers

- Einfaches initiales Setup
  - Anmeldung: Erster Account hat Admin-Rechte
- Anlegen erster Spaces und Artikel
- Freigabe der Plattform für Anwender

3.3 Angedachter Lösungsweg der Challenge

Ausnutzen der platzierten Schwachstellen innerhalb der Anwendung

- Enumerieren der vorhandenen Artikel
- Auslesen der Meta-Daten (Spaces & Space-ID, Autoren und Autoren-ID)
- Rechte-Ausweitung innerhalb der Anwendung durch selbst-hinzufügen zu Administrator-Space, an der GUI vorbei, ermöglicht durch fehlende Autorisationsprüfung

Ausnutzen des initialen Setup-Modus

- Löschen aller Anwender
- Im Initialen Modus neuen Account
- mit diesem in die Administartions-Datenbank

3.3.1 Tipps und Hinweise für Lösungsweg

- Der erste Beitrag, der sichtbar ist, hat die ID 2
  - Hinweis darauf, dass es einen Eintrag mit der ID 1 geben müsste.
- Der erste Beitrag (ID 1) ist eine vom (simulierten Admin) angelegte Notiz an andere Admins
  - Der Admin drückt Freude darüber aus, wie einfach das initiale Setup dadurch war, dass das System einfach dem ersten User-Account Administrationsrechte gibt.

3.4 Realitätsbezug

2024 September: KIA

- News
  - Spiegel: Hacker konnten koreanische Autos per App orten, starten, hupen lassen
  - Heise: Kia: Lücken in Webportal erlaubten Forschern Fernzugriff auf Autos
  - Der Standard: Schwere Sicherheitslücken bei Kia ermöglichten Fernortung und Start von Millionen Autos
- Blog (Originalquelle)
  - Sam Curry: Hacking Kia: Remotely Controlling Cars With Just a License Plate

TODO: da werden sich schon noch Beispiele finden lassen

3.5 Beta-Test

Hamburger CTF-Team Cyclopropenylidene (C3H2)

- Feedback: ID für ersten sichtbaren Artikel sollte 2 sein, als Hinweis darauf, dass es einen weiteren Artikel (ID 1) gibt.
  - -> so umgesetzt
- Technisches Problem aufgedeckt: Ein Beta-Tester hat nicht nur einen Account angelegt und diesem (wie angedacht) einen Account Zugriff auf den versteckten Space gegeben, sondern mit Hilfe eines http replay Proxy die Sicherheitslücke so ausgenutzt, dass alle Accounts Zugriff auf den versteckten Space hatten. das hat dafür gesorgt, dass eine Beta-Testerin, die sich zuvor einen Account angelegt hat, aber die Sicherheitslücke noch nicht gefunden hat, plötzlich ohne eigenes zutun Zugriff auf den versteckten Space hatte.

- -> Gelernt: Diese Challenge muss pro Person/Team als eigene Instanz bereitgestellt werden.

3.6 Durchführung Workshop

- Workshop Week an HAW September 2024
  - ca. 12 Teilnehmende
  - Studierende
    - Informatik
      - Bachelor
      - Master
    - Sonstige
  - Evaluationsbögen
    - TODO: Ergebnis der Evaluationsbügen nutzbar?? (Jedenfalls nicht für direkten Vergleich!) (Eventuell noch ein Workshop notwendig??)
- IT-Security Konferenz „Nights of open Knowledge“ (NOOK)
  - 34 Teilnehmende
  - Allgemeines Feedback
    - Skala:
      - „auf jeden Fall“ / „eher ja“ / „eher nein“ / „auf keinen Fall“
    - Antworten
      - „War der Vortrag interessant?“
        - 12/12: „auf jeden Fall“
      - „Hat der Vortragende das Thema beherrscht?“
        - 12/12: „auf jeden Fall“
      - „Konnten Fragen beantwortet werden?“
        - 9/12 „auf jeden Fall“
        - 3/12 „eher ja“
      - „War das Material (Folien u.ä.) ansprechend?“
        - 10/12 „auf jeden Fall“
        - 2/12 „eher ja“
  - Es hat keine inhaltliche Evaluation stattgefunden

4 Ergebnis

4.1 Evaluation

TODO: Die entstandene Challenge so evaluieren wie in [5] beschrieben.

- semi-strukturierte Interviews ()
- Feedbackbogen (was hat gut funktioniert, was nicht)
- Fragebogen, Evaluationsfragen

Direkter Vergleich des Ergbenis der EIGENEN Challenge mit den Challenges aus dem Requirements-Paper [5]

Index	Requirement	Evaluation
1	Have a clearly defined learning goal objective	todo
2	Adapted to background (job description) of participants developers	todo
3	Well defined working mechanics (e.g. which tools to use or what to do)	todo
4	Defined and progressive level of difficulty challenges	todo
5	Elicit discussions of the solutions (e.g. is there a better/simpler way to solve?)	todo
6	Provide possible solution after challenge solved	todo
7	Adapted to the skill level of participants	todo
8	Challenge includes hint that aid to arrive to the solution	todo
9	Clear, standardized and simple solution (not based on obscure knowledge)	todo
10	Planned duration of the exercise	todo
11	Explains issues arriving from interplay of different technologies or components	todo
12	Adapted to company internal secure coding guidelines and policies	todo
13	Challenges are put from the defensive perspective	todo
14	Solutions does not require specific knowledge of hacking tools	todo
15	Challenges should raise awareness on possible consequences of malicious attack	todo
		?? %

Tabelle 1: Evaluationsergebnis

- Ergebnis (hoffentlich): meine Challenge erfüllt die Anforderungen besser

4.2 Diskussion

Die Evaluation zeigt, dass

- …?
- Zielgrupopenorientiertheit (zugeschnitten auf Jobtitle) weiterhin schwierig
- … ?

- Challenges are put from the defensive perspective
  - not fulfilled??
- ...?

5 Fazit

. . .

5.1 Ausblick

Durch einen „import“ anderer „Modelle“ aus dem Unterhaltungsbereich könnten „Empfehlungen für Verbesserungen und Erkenntnisse zur Gestaltung und Entwicklung effektiverer SG [Serious Games]“ übernommen werden [10]

Die durchgeführte Evaluation sowohl der bestehenden CTF-Events als auch der entwickelten Challenge ist ausbaufähig.

Ein konkretes Beispiel für die Übernahme von bestehenden Methoden aus der Unterhaltungsmedien-Entwicklung könnte ergänzend oder anstelle der durchgeführten Evaluation Evaluations-Methoden aus der allgemeinen Spiele-Entwicklung oder dem Übergeordneten Feld der „serious games“ auch auf die entwickelte/n Challenge/s adaptiert werden. Ansätze hierfür finden sich zum Beispiel in [User Experience Evaluation Methods for Games in Serious Contexts] [11] oder [Framework for evaluating Capture the Flag (CTF) security competitions] [12]

Wird das Feedback der Teilnehmenden ernst genommen und liefern die Evaluations-Methoden gute Einblicke, lassen sich die somit ermittelte Erfahrungen wieder als Anforderungen formulieren, um die bestehenden Anforderungen zu verfeinern oder zu ergänzen.

Bibliographie

[1] L. W. Anderson und D. R. Krathwohl, Hrsg., „A taxonomy for learning, teaching, and assessing: a revision of Bloom's taxonomy of educational objectives“. Longman, New York, 2001.

[2] M. T. H. Chi und R. Wylie, „The ICAP Framework: Linking Cognitive Engagement to Active Learning Outcomes“, *Educational Psychologist*, Bd. 49, Nr. 4, S. 219–243, Okt. 2014, doi: 10.1080/00461520.2014.965823.

[3] G. Costa und M. Ribaudo, „Designing a Serious Game for Cybersecurity Education“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 265–290, 2023. doi: 10.1007/978-3-031-33338-5_12.

[4] K. M. L. Cooper und A. Bucchiarone, Hrsg., „Software Engineering for Games in Serious Contexts“. Springer Nature Switzerland, Cham, 2023. doi: 10.1007/978-3-031-33338-5_12.

[5] T. Espinha Gasiba, K. Beckers, S. Suppan, und F. Rezabek, „On the Requirements for Serious Games Geared Towards Software Developers in the Industry“, in *2019 IEEE 27th International Requirements Engineering Conference (RE)*, Jeju Island, Korea (South): IEEE, Sep. 2019, S. 286–296. doi: 10.1109/RE.2019.00038.

[6] J. Eckstein, J. Bergin, und H. Sharp, „Patterns for active learning“, in *Proceedings of PLOP*, 2002.

[7] „CTFtime.org / What is Capture The Flag?“. Zugegriffen: 24. Februar 2025. [Online]. Verfügbar unter: https://ctftime.org/ctf-wtf/

[8] Computer Science Department, Texas Tech University, A. Siami Namin, Z. Aguirre-Muñoz, Texas Tech University, K. Jones, und Texas Tech University, „Teaching Cyber Security through Competition An Experience Report about a Participatory Training Workshop“, in *7th Annual International Conference on Computer Science Education: Innovation & Technology (CSEIT 2016)*, Global Science & Technology Forum (GSTF), Okt. 2016. doi: 10.5176/2251-2195_CSEIT16.39.

[9] K. Leune und S. J. Petrilli, „Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education“, in *Proceedings of the 18th Annual Conference on Information Technology Education*, Rochester New York USA: ACM, Sep. 2017, S. 47–52. doi: 10.1145/3125659.3125686.

[10] V. Wanick, J. Stallwood, und G. Xavier, „Future Directions in Games for Serious Contexts: A Conversation About Transferability“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 137–153, 2023. doi: 10.1007/978-3-031-33338-5_7.

[11] S. Kirginas, „User Experience Evaluation Methods for Games in Serious Contexts“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 19–42, 2023. doi: 10.1007/978-3-031-33338-5_2.

[12] R. Raman, S. Sunny, V. Pavithran, und K. Achuthan, „Framework for evaluating Capture the Flag (CTF) security competitions“, in *International Conference for Convergence for Technology-2014*, Pune, India: IEEE, Apr. 2014, S. 1–5. doi: 10.1109/I2CT.2014.7092098.